This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (Currently Amended): A method for protected execution of a cryptographic calculation, in which a key with at least two key parameters is drawn on, wherein the key is a private RSA key for use in an RSA method, wherein each key parameter is a private RSA key parameter contained in the private RSA key, wherein an integrity check of the private RSA key is performed in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second private RSA key parameter by corrupting at least one first private RSA key parameter, wherein the cryptographic calculation is one of a decryption in the RSA method and a signature generation in the RSA method, and wherein each operation of the method for protected execution of the cryptographic calculation is executed by an integrated circuit.

Claims 2-13 (Canceled).

Claim 14 (Currently Amended): The method as claimed in claim 1, wherein in the integrity check it is determined whether the value of at least one private RSA key parameter is contained in a range of valid values, wherein the range is non-contiguous in that it has a plurality of gaps.

Claim 15 (Currently Amended): The method as claimed in claim 1, wherein in the integrity check it is determined whether at least two private RSA key parameters are in a predetermined relationship to one another.

Claim 16 (Previously Presented): The method as claimed in claim 1, wherein the integrity check includes a multiplicative operation, in particular a divisibility test.

Claim 17 (Currently Amended): The method as claimed in claim 1, wherein in the integrity check it is checked whether at least one of the private RSA key parameters is evenly divisible by a safeguard value.

Claim 18 (Currently Amended): The method as claimed in claim 1, wherein in the integrity check it is checked whether at least one value which differs from one of the private RSA key parameters by a multiple of a safeguard value is evenly divisible by the safeguard value.

Claim 19 (Currently Amended): The method as claimed in claim 1, wherein in the integrity check a checksum stored with the private RSA key parameters is compared with a checksum newly calculated after passing of the private RSA key parameters.

Claim 20 (Previously Presented): The method as claimed in claim 1, wherein, to check the integrity, important parameters to be passed are multiply passed and checked for identity after passing.

Claim 21 (Canceled).

Claim 22 (Previously Presented): The method as claimed in claim 1, wherein the RSA method is an RSA-CRT method.

Claim 23 (Previously Presented): The method as claimed in claim 1, wherein in the cryptographic calculation at least one exponentiation operation is performed and in the integrity check it is checked whether the exponent used in the exponentiation operation is evenly divisible by a safeguard value.

Claim 24 (Previously Presented): The method as claimed in claim 23, wherein in the cryptographic calculation an exponent blinding method is applied for protection against spying.

Claim 25 (Previously Presented): The method as claimed in claim 1, wherein the prime factors of the RSA method are multiplied by a masking parameter and an error freedom of the calculation sequence is checked by an equality check modulo the masking parameter.

Claim 26 (Currently Amended): The method as claimed in claim 1, wherein at least one private RSA key parameter is the product of a value required for the cryptographic calculation times a safeguard value, and wherein the integrity check includes a divisibility check.

Claim 27 (Currently Amended): A method for determining a key for a cryptographic calculation with at least two key parameters, wherein the key is a private RSA key for use in an RSA method, and wherein each key parameter is a private RSA key parameter contained in the private RSA key, the key being adapted to be used in a method for protected execution of a cryptographic calculation wherein an integrity check of the private RSA key is performed in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second private RSA key parameter by corrupting at least one first private RSA key parameter, wherein the cryptographic calculation is one of a decryption in the RSA method and a

signature generation in the RSA method, and wherein each operation of the method for determining the private RSA key for the cryptographic calculation is executed by an integrated circuit.

Claim 28 (Currently Amended): The method as claimed in claim 27, wherein at least one private RSA key parameter is obtained by multiplication of a value required for the cryptographic calculation by a safeguard value.

Claim 29 (Currently Amended): The method as claimed in claim 27, wherein at least one private RSA key parameter is the product of a value required for the cryptographic calculation times a safeguard value, and wherein the integrity check includes a divisibility check.

Claim 30 (Currently Amended): A computer program product including a computer-readable storage medium, the computer readable storage medium being a physical medium and having a computer program stored thereon, the computer program including program commands to cause a processor to execute a method for protected execution of a cryptographic calculation, in which a key with at least two key parameters is drawn on, wherein the key is a private RSA key for use in an RSA method, wherein each key parameter is a private RSA key parameter contained in the private RSA key, wherein an integrity check of the private RSA key is performed in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second private RSA key parameter by corrupting at least one first private RSA key parameter, and wherein the cryptographic calculation is one of a decryption in the RSA method and a signature generation in the RSA method.

Claim 31 (Currently Amended): The computer program product as claimed in claim 30, wherein at least one private RSA key parameter is the product of a value required for the cryptographic calculation times a safeguard value, and wherein the integrity check includes a divisibility check.

Claim 32 (Currently Amended): A portable data carrier comprising a processor and a storage, the storage having a computer program stored thereon, the computer program including program commands to cause the processor to execute a method for protected execution of a cryptographic calculation, in which a key with at least two key parameters is drawn on, wherein the key is a private RSA key for use in an RSA method, wherein each key parameter is a private RSA key parameter contained in the private RSA key, wherein an integrity check of the private RSA key is performed in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second private RSA key parameter by corrupting at least one first private RSA key parameter, wherein the data carrier is one of a smart card and a chip module, and wherein the cryptographic calculation is one of a decryption in the RSA method and a signature generation in the RSA method.

Claim 33 (Canceled).

Claim 34 (Currently Amended): The portable data carrier as claimed in claim 32, wherein at least one private RSA key parameter is the product of a value required for the cryptographic calculation times a safeguard value, and wherein the integrity check includes a divisibility check.